PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-232442
(43)Date of publication of application : 22.08.2000

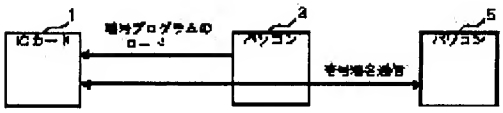
(51)Int.Cl. H04L 9/10
G09C 1/00
H04L 9/14

(21)Application number : 11-030861
(22)Date of filing : 09.02.1999

(71)Applicant : NTT DATA CORP
(72)Inventor : HAYASHI SEIICHIRO

(54) INFORMATION PROCESSING METHOD/SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To execute all enciphered programs that can be used and to secure the storage area of an application program even in the information processor of comparatively small storage capacity.
SOLUTION: The read-only memory of an IC card 1 stores a secret key for enciphering, an enciphering system identification flag, a verification identification flag, and a verification program. The enciphering system identification flag and the verification identification flag are transmitted to a personal computer 3. An enciphered program from the personal computer 3 is received and the authenticity of the program is verified by identifying signature information from the personal computer 3 by the verification program. The read-only memory of the personal computer 3 previously stores an enciphered program group and a signature information group. The IC card 1 selects an enciphering system used for cipher/signature communication with the check of the enciphering system identification flag and the enciphered program corresponding to the enciphering system is extracted from a enciphered program group so as to transmit it to the IC card 1. Signature information corresponding to the enciphered program selected/extracted from the enciphered program group on the basis of the check of the enciphering system identification flag is selected/extracted from the signature information group and it is transmitted to the IC card 1.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－232442
（P2000－232442A）
(43)公開日　平成12年８月22日(2000.8.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ	９Ａ００１
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	

審査請求　未請求　請求項の数11　ＯＬ　（全６頁）

(21)出願番号　特願平11－30861

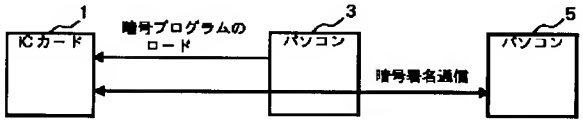
(22)出願日　平成11年２月９日(1999.2.9)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　林　誠一郎
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095371
弁理士　上村　輝之

Ｆターム(参考)　5J104 AA01 AA08 AA32 LA03 NA27
NA35 NA38 PA07
9A001 BB02 BB03 BB04 CC02 DD08
DD10 EE03 FZ01 JJ18 KZ56
LL03

(54)【発明の名称】　情報処理方法及びシステム

(57)【要約】
【課題】　比較的記憶容量の小さな情報処理装置でも、使用可能な全ての暗号プログラムを実行でき、応用プログラムの記憶領域をも確保できるようにする。
【解決手段】　ＩＣカード１の読出し専用メモリは、暗号化のための秘密鍵、暗号方式識別フラグ、検証識別フラグ、検証プログラムを記憶する。暗号方式識別フラグ、検証識別フラグはパソコン３に送信される。パソコン３からの暗号プログラムを受信し、その正当性をパソコン３からの署名情報を検証プログラムで識別することにより検証する。パソコン３の読出し専用メモリは、暗号プログラム群、署名情報群を予め記憶する。暗号方式識別フラグのチェックにより、ＩＣカード１が暗号・署名通信に用いる暗号方式を選択し、その暗号方式に対応する暗号プログラムを暗号プログラム群中から抽出してＩＣカード１に送信する。ＩＣカード１からの検証識別フラグのチェックにより、暗号方式識別フラグのチェックに基づいて暗号プログラム群から選択、抽出した暗号プログラムに対応する署名情報を、署名情報群の中から選択、抽出してＩＣカード１に送信する。



【特許請求の範囲】

【請求項１】　情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、
前記第２の情報処理装置が、複数種類の暗号プログラムを保持し、前記第１の情報処理装置からの要求に基づいて前記複数種類の暗号プログラム中より対応するものを選択して前記第１の情報処理装置に与える情報処理システム。

【請求項２】　請求項１記載の情報処理システムにおいて、
前記第２の情報処理装置が、前記第１の情報処理装置が有するメモリよりも記憶容量の大きなメモリを有する情報処理システム。

【請求項３】　請求項１記載の情報処理システムにおいて、
前記第１の情報処理装置が、ＩＣカード又はＰＣＭＣＩＡカードであり、前記第２の情報処理装置が、パーソナルコンピュータである情報処理システム。

【請求項４】　請求項１記載の情報処理システムにおいて、
前記第２の情報処理装置が、複数種類の暗号プログラムと共に、前記各暗号プログラムに対応する複数種類の署名情報をも保持する情報処理システム。

【請求項５】　請求項１記載の情報処理システムにおいて、
前記第１の情報処理装置が、予め保持する、前記暗号プログラムを識別するための情報を前記第２の情報処理装置に送り、前記第２の情報処理装置がその情報に基づいて前記複数種類の暗号プログラム中より対応するものを選択して前記第１の情報処理装置に与える情報処理システム。

【請求項６】　請求項４又は請求項５記載の情報処理システムにおいて、
前記第１の情報処理装置が、前記第２の情報処理装置から暗号プログラを受けたとき、それに対応する署名情報を前記第２の情報処理装置が前記複数種類の署名情報から選択するのに必要な情報を、前記第２の情報処理装置に送る情報処理システム。

【請求項７】　請求項１記載の情報処理システムにおいて、
前記第１の情報処理装置が、前記第２の情報処理装置から与えられる暗号プログラムの正当性を検証するための手段を更に有する情報処理システム。

【請求項８】　請求項７記載の情報処理システムにおいて、
前記検証手段が、前記第２の情報処理装置から与えられる署名情報を識別することにより、前記暗号プログラムの正当性を検証する情報処理システム。

【請求項９】　請求項７又は請求項８記載の情報処理システムにおいて、
前記第１の情報処理装置が、前記検証手段により正当性を検証された暗号プログラムと、予め内蔵する秘密鍵とにより情報を暗号化する情報処理システム。

【請求項１０】　情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、
前記第１の情報処理装置が、前記第２の情報処理装置に暗号プログラムを要求する第１の過程と、
前記第２の情報処理装置が、前記要求に基づいて保持している複数種類の暗号プログラムの中から対応するものを選択して前記第１の情報処理装置に与える第２の過程と、
を有する情報処理方法。

【請求項１１】　情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、
前記第２の情報処理装置が、複数種類の暗号プログラムを保持し、前記第１の情報処理装置からの要求に基づいて前記複数種類の暗号プログラム中より対応するものを選択して前記第１の情報処理装置に与える情報処理システムにおける前記各情報処理装置としてコンピュータを動作させるためのコンピュータプログラムを担持したコンピュータ読取可能なプログラム媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理方法及びシステムに関するものである。

【０００２】

【従来の技術】従来、情報処理装置同士の間で情報の授受を暗号通信により行う場合、予め各情報処理装置の読出し専用メモリに保存しておいた複数の暗号プログラムの中から対応するものを適宜選択し、その選択した暗号プログラムを、各情報処理装置において実行する手法で対処していた。

【０００３】

【発明が解決しようとする課題】ところで、上述した手法では、複数の暗号プログラムを各情報処理装置の、プログラムや情報の改竄がし難いとされる読出し専用メモリに予め保存しておくため、上記暗号プログラムの信頼性が高く、正当な暗号プログラムにより適正に情報の暗号通信が行えるという利点がある。

【０００４】しかし、情報処理装置が、例えばＩＣカードやＰＣＭＣＩＡカードのような比較的小規模な情報処理装置である場合には、それに応じて読出し専用メモリの記憶容量も当然小さなものにならざるを得ない。そのため、使用が想定され得る複数の暗号プログラムを全て保存しようとすると、上記メモリでは、例えば応用プログラム（アプリケーションプログラム）を保存するための記憶容量が不足するという問題が生じる。また、上記

メモリにおいて、応用プログラムの記憶領域を確保しようとすれば、上記暗号プログラムを全て保存するための記憶容量が不足することになり、保存できるプログラムが制限されるという問題が生じる。

【０００５】従って本発明の目的は、比較的記憶容量の小さな情報処理装置を用いる場合でも、使用が想定され得る全ての暗号プログラムを実行することができ、且つ、応用プログラムの記憶領域をも確保できるようにすることにある。

【０００６】

【課題を解決するための手段】本発明の第１の側面に従う情報処理システムは、情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、第２の情報処理装置が、複数種類の暗号プログラムを保持し、第１の情報処理装置からの要求に基づいて複数種類の暗号プログラム中より対応するものを選択して第１の情報処理装置に与える。

【０００７】上記構成によれば、第２の情報処理装置が、第１の情報処理装置からの要求に基づいて、保持している複数種類の暗号プログラム中より対応するものを選択して第１の情報処理装置に与える。そのため、第１の情報処理装置が比較的記憶容量の小さな情報処理装置であっても、使用が想定され得る全ての暗号プログラムを実行することができ、応用プログラムの記憶領域をも確保できる。

【０００８】本発明の第１の側面に係る好適な実施形態では、第２の情報処理装置は、第１の情報処理装置が有するメモリよりも記憶容量の大きなメモリを有する。例えば、第１の情報処理装置としてはＩＣカード又はＰＣＭＣＩＡカードが挙げられ、第２の情報処理装置としてはパーソナルコンピュータが挙げられる。

【０００９】また、上記実施形態では、第２の情報処理装置は複数種類の暗号プログラムと共に、各暗号プログラムに対応する複数種類の署名情報をも保持する。第１の情報処理装置は、予め保持する、暗号プログラムを識別するための情報（例えば、暗号方式識別フラグ）を第２の情報処理装置に送り、第２の情報処理装置がその情報に基づいて複数種類の暗号プログラム中より対応するものを選択して第１の情報処理装置に与える。

【００１０】また、上記実施形態では、第１の情報処理装置が、第２の情報処理装置から暗号プログラムを受けたとき、それに対応する署名情報を第２の情報処理装置が複数種類の署名情報から選択するのに必要な情報（検証識別フラグ）を、第２の情報処理装置に送るようになっている。第１の情報処理装置は、第２の情報処理装置から与えられる暗号プログラムの正当性を検証するための手段（例えば、検証プログラム）を更に有する。この検証手段は、第２の情報処理装置から与えられる署名情報を識別することにより、暗号プログラムの正当性を検証する。更に、第１の情報処理装置は、検証手段により正当性を検証された暗号プログラムと、予め内蔵する秘密鍵とにより情報を暗号化する。

【００１１】本発明の第２の側面に従う情報処理方法は、情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、第１の情報処理装置が、第２の情報処理装置に暗号プログラムを要求する第１の過程と、第２の情報処理装置が、その要求に基づいて保持している複数種類の暗号プログラムの中から対応するものを選択して第１の情報処理装置に与える第２の過程とを有する。

【００１２】本発明の第３の側面に従うプログラム媒体は、情報を暗号化して送信する第１の情報処理装置と、この第１の情報処理装置とは別の第２の情報処理装置とを備え、第２の情報処理装置が、複数種類の暗号プログラムを保持し、第１の情報処理装置からの要求に基づいて複数種類の暗号プログラム中より対応するものを選択して第１の情報処理装置に与える情報処理システムにおける各情報処理装置としてコンピュータを動作させるためのコンピュータプログラムをコンピュータ読取可能に担持する。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１４】図１は、本発明の一実施形態に係る情報処理システムの全体構成を示すブロック図である。

【００１５】上記システムは、図１に示すように、比較的小規模な情報処理装置の一例としてのＩＣカード１と、比較的大規模な情報処理装置の一例としての複数台のパーソナルコンピュータ（パソコン）３、５とを備える。

【００１６】ＩＣカード１は、パソコン３にセッティングされることで、パソコン３との間で必要なプログラムや各種情報の授受を行う。ＩＣカード１の読出し専用メモリ（図示しない）には、暗号化のための秘密鍵（図示しない）を始め、暗号方式識別フラグ（図２に示す）や、検証識別フラグ（図３に示す）等が予め格納される。上記メモリには、更に、検証プログラム（又は署名検証プログラム）（図示しない）も格納される。この検証プログラムとしては、例えば上記秘密鍵等と同様に予め上記メモリに格納される署名検証暗号プログラムか、或いはパソコン３との間での通信中にパソコン３から与えられ、上記メモリに格納される署名検証暗号プログラム等が挙げられる。

【００１７】上記暗号方式識別フラグ、及び上記検証識別フラグは、パソコン３からの送信要求に応じてＩＣカード１からパソコン３に夫々送信される。ＩＣカード１は、また、パソコン３から送信された暗号プログラムを受信して上記メモリに格納しておき、上記暗号プログラムとは別にパソコン３から送信された上記暗号プログラムに対応する署名情報を、上記検証プログラムを用いて

識別することにより、上記暗号プログラムの正当性を検証する。ＩＣカード１は、更に、上記暗号プログラムの正当性が検証されたとき、その暗号プログラムと上記秘密鍵とに基づき、パソコン５に送信すべき情報をＩＣカード１内において暗号化すると共に暗号化した情報を、パソコン３を介してパソコン５に送信する。

【００１８】パソコン３は、上述したように、ＩＣカード１がセッティングされることでＩＣカード１との間で必要なプログラムや各種情報の授受を行うのみならず、ＩＣカード１とパソコン５との間で行われる暗号・署名通信を媒介する。パソコン３の読出し専用メモリ（図示しない）には、ＩＣカード１に送信するための暗号プログラム群や、各々の暗号プログラムに対応して設定される署名情報群（いずれも、図４に示す）等が予め格納される。上記メモリには、必要に応じて上述した検証プログラム（つまり、署名検証暗号プログラム）が格納される場合もある。

【００１９】パソコン３は、ＩＣカード１からの暗号方式識別フラグをチェックすることにより、ＩＣカード１がパソコン５との間で行う暗号・署名通信に用いる暗号方式を選択し、この選択した暗号方式に対応する暗号プログラムを上述した暗号プログラム群の中から抽出してＩＣカード１に送信する。パソコン３は、また、ＩＣカード１から送信された検証識別フラグをチェックすることにより、上記暗号方式識別フラグのチェックに基づいて上記暗号プログラム群から選択、抽出した暗号プログラムに対応する署名情報を、上述した署名情報群の中から選択、抽出してＩＣカード１に送信する。パソコン３は、更に、ＩＣカード１とパソコン５との間で行われる暗号・署名通信を媒介する。

【００２０】パソコン５は、上述したように、パソコン３を媒介としてＩＣカード１との間で暗号・署名通信を行う。

【００２１】図２は、図１に記載したＩＣカード１が保持する暗号方式識別フラグを示す説明図である。

【００２２】暗号方式識別フラグ７は、上述したように、ＩＣカード１からパソコン３に送信され、暗号・署名通信においてＩＣカード１が使用する暗号方式を選択するためにパソコン３によりチェックされるもので、図２に示すように、暗号方式識別コード９と、版情報１１と、鍵長１３とを備える。上記チェックにより、いずれかの暗号方式が選択され、その選択された暗号方式に対応する暗号プログラムが、上述した暗号プログラム群の中から抽出される。

【００２３】暗号方式識別コード９は、ＦＥＡＬ（ファースト・エンクリプション・アルゴリズム）、ＤＥＳ（データ・エンクリプション・スタンダード）、ＲＳＡ（リベスト・シャミール・アドルマン）、及びＥＳＩＧＮ（エレクトリック・シグネチャー）等の暗号方式を識別するためのコードである。

【００２４】版情報１１とは、上述した各暗号方式識別コード９に係るバージョン情報である。

【００２５】鍵長１３とは、暗号に使用する鍵のビット長を示している。

【００２６】図３は、図１に記載したＩＣカード１が保持する検証識別フラグを示す説明図である。

【００２７】検証識別フラグ１５は、上述したように、ＩＣカード１からパソコン３に送信され、パソコン３によりチェックされるもので、図３に示すように、検証方式識別コード１７と、版情報１９と、鍵長２１とを備える。上記チェックにより、上述した暗号方式識別フラグ７のチェックに基づき、上記暗号プログラム群の中から選択、抽出された暗号プログラムに対応する署名情報が、上記署名情報群の中から選択、抽出される。

【００２８】検証方式識別コード１７は、ＲＳＡ署名情報及びＥＳＩＧＮ署名情報等の署名情報が、上記各暗号方式（各暗号プログラムＦＥＡＬ、ＤＥＳ、ＲＳＡ、ＥＳＩＧＮ）のいずれに属するかを識別するためのコードである。

【００２９】版情報１９とは、検証方式識別コード１７のバージョン情報である。

【００３０】鍵長２１とは、上述した鍵長１３におけると同様、暗号に使用する鍵のビット長を示している。

【００３１】図４は、図１に記載したパソコン３が保持する暗号プログラム群及びそれらに対応する署名情報群を示す説明図である。

【００３２】図４に示すように、暗号プログラム群２３は、ＦＥＡＬプログラム２７と、ＤＥＳプログラム２９と、ＲＳＡプログラム３１と、ＥＳＩＧＮプログラム３３とを含む。署名情報群２５は、上記各暗号プログラム（２７～３３）に夫々対応して設定される複数の署名情報、即ち、ＲＳＡ署名情報３５及びＥＳＩＧＮ署名情報３７から構成される。なお、署名情報群２５を構成する署名情報の種類は、上記ＲＳＡ署名情報３５及びＥＳＩＧＮ署名情報３７のみに限定されるものではなく、例えば図３に示した鍵長２１の長さに応じて、更に別の種類の署名情報が追加され得る。

【００３３】暗号プログラム群２３に含まれる各暗号プログラム（２７～３３）のいずれかは、ＩＣカード１から暗号方式識別フラグ７がパソコン３に送信されたことに起因してパソコン３により読出され、ＩＣカード１に送信される。また、署名情報群２５を構成するＲＳＡ署名情報３５及びＥＳＩＧＮ署名情報３７のいずれかは、ＩＣカード１から検証識別フラグ１５がパソコン３に送信されたことに起因してパソコン３により読出され、ＩＣカード１に送信される。

【００３４】図５は、図１に記載した情報処理システムにおける各部の処理流れを示す説明図である。

【００３５】図５において、ＩＣカード１がパソコン３にセッティングされると、ＩＣカード１は、まず、パソ

コン３からの送信要求に応じて暗号方式識別フラグ７をパソコン３に送信する（ステップＳ４１）。パソコン３側では、受信した暗号方式識別フラグ７をチェックすることにより（ステップＳ４２）、ＩＣカード１がパソコン５との間で行う暗号・署名通信に用いる暗号方式を選択する。そして、この選択した暗号方式に対応する暗号プログラムを上述した暗号プログラム群の中から抽出し（ステップＳ４３）、ＩＣカード１に送信する（ステップＳ４４）。

【００３６】ＩＣカード１側では、受信した暗号プログラムを読出し専用メモリに格納すると共に（ステップＳ４５）、パソコン３からの送信要求に応じて検証識別フラグ１５をパソコン３に送信する（ステップＳ４６）。パソコン３側では、受信した検証識別フラグ１５をチェックすることにより（ステップＳ４７）、上記暗号方式識別フラグ７のチェックに基づいて上記暗号プログラム群２３から選択、抽出した暗号プログラムに対応する署名情報を、上述した署名情報群２５の中から選択、抽出する（ステップＳ４８）。そして、その署名情報を、ＩＣカード１に送信する（ステップＳ４９）。

【００３７】ＩＣカード１側では、受信した署名情報を、上記検証プログラムを用いて識別することにより、上記メモリに格納した暗号プログラムの正当性を検証する（ステップＳ５０）。この結果、上記暗号プログラムの正当性が検証されると、ＩＣカード１は、その暗号プログラムと上述した暗号化の秘密鍵とに基づき、パソコン５に送信すべき情報をＩＣカード１内において暗号化すると共に、暗号化した情報をパソコン３を介してパソコン５に送信する（ステップＳ５１）。これにより、一連の処理動作が終了する。

【００３８】以上説明したように、本発明の一実施形態によれば、ＩＣカード１が使用することを想定した複数種類の暗号プログラムを、パソコン３の読出し専用メモリに格納するため、ＩＣカード１の読出し専用メモリも記憶容量の大きさ如何に拘らず、ＩＣカード１は多数の暗号プログラムを使用することができる。しかも、ＩＣカード１の読出し専用メモリの記憶領域が上記多数の暗号プログラムによって占有されることがないため、ＩＣカード１の読出し専用メモリに応用プログラムを格納することも可能である。

【００３９】上述した内容は、あくまで本発明の一実施＊形態に係るものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。

【００４０】

【発明の効果】以上説明したように、本発明によれば、比較的記憶容量の小さな情報処理装置を用いる場合でも、使用が想定され得る全ての暗号プログラムを実行することができ、且つ、応用プログラムの記憶領域をも確保できるようにすることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る情報処理システムの全体構成を示すブロック図。

【図２】図１に記載のＩＣカードが保持する暗号方式識別フラグを示す説明図。

【図３】図１に記載のＩＣカードが保持する検証識別フラグを示す説明図。

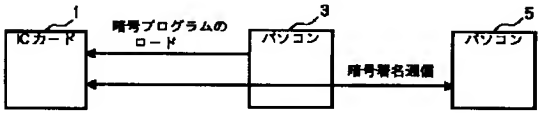
【図４】図１に記載のパーソナルコンピュータ（パソコン）が保持する暗号プログラム群及びそれらに対応する署名情報群を示す説明図。

【図５】図１に記載のシステムにおける各部の処理流れを示す説明図。

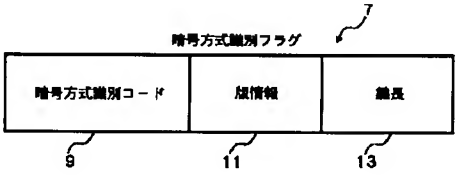
【符号の説明】

１　ＩＣカード
３、５　パーソナルコンピュータ（パソコン）
７　暗号方式識別フラグ
９　暗号方式識別コード
１１、１９　版情報
１３、２１　鍵長
１５　検証識別フラグ
１７　検証方式識別コード
２３　暗号情報群
２５　署名情報群
２７　ＦＥＡＬ（ファースト・エンクリプション・アルゴリズム）プログラム
２９　ＤＥＳ（データ・エンクリプション・スタンダード）プログラム
３１　ＲＳＡ（リベスト・シャミール・アドルマン）プログラム
３３　ＥＳＩＧＮ（エレクトリック・シグネチャー）プログラム
３５　ＲＳＡ署名情報
３７　ＥＳＩＧＮ署名情報

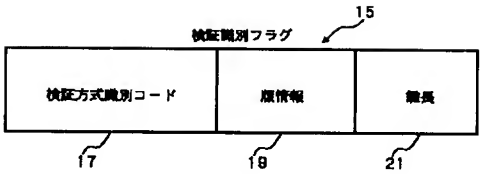
【図１】



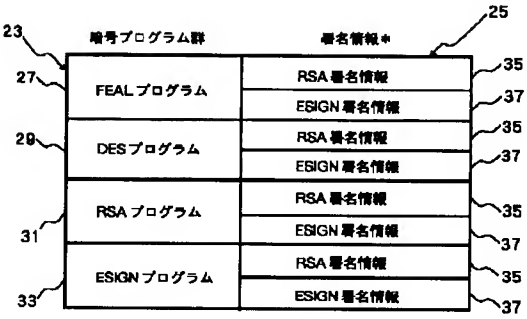
【図２】



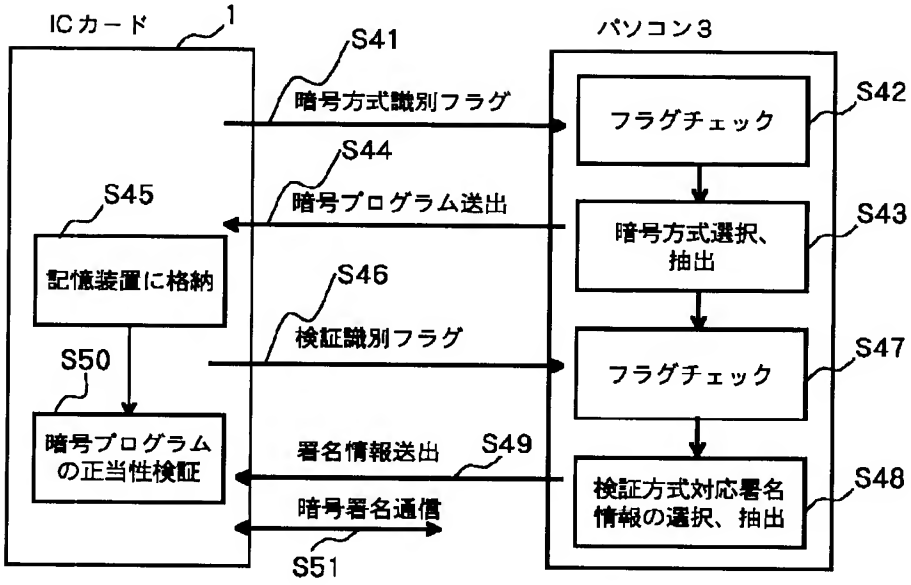
【図３】


15
検証識別フラグ
検証方式識別コード
版情報
鍵長
17
19
21

【図４】


23
暗号プログラム群
署名情報*
25
27
FEAL プログラム
RSA 署名情報
ESIGN 署名情報
35
37
29
DES プログラム
RSA 署名情報
ESIGN 署名情報
35
37
31
RSA プログラム
RSA 署名情報
ESIGN 署名情報
35
37
33
ESIGN プログラム
RSA 署名情報
ESIGN 署名情報
35
37

【図５】


ICカード
1
パソコン３
S41
暗号方式識別フラグ
S42
フラグチェック
S44
暗号プログラム送出
S43
暗号方式選択、抽出
S45
記憶装置に格納
S46
検証識別フラグ
S47
フラグチェック
S50
暗号プログラムの正当性検証
署名情報送出
S49
S48
検証方式対応署名情報の選択、抽出
暗号署名通信
S51